Deutscher Bundestag **Drucksache 17/6972**

17. Wahlperiode 09. 09. 2011

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Wolfgang Wieland, Memet Kilic, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 17/6849 –

Datensicherheit und Datenschutz bei Zoll und Bundespolizei

Vorbemerkung der Fragesteller

Anfang Juli dieses Jahres wurde bekannt, dass ein Hacker-Angriff auf Server des Zolls erfolgte. Eine Gruppe mit Namen „No-Name-Crew“ war dabei offenbar in den Besitz von Daten des Zolls gelangt und hatte diese anschließend im Internet veröffentlicht. Zu den veröffentlichten Daten sollen Klarnamen von Fahndern und observierten Tatverdächtigen, Kraftfahrzeugkennzeichen ausgespähter Fahrzeuge und die Passwörter von Peilsendern der Ermittler zählen. Auch Daten des Zielverfolgungssystems Patras sollen von den Veröffentlichungen betroffen gewesen sein. Zwischenzeitlich liegen dazu weitere, teilweise widersprüchliche Medienberichte vor. „FOCUS Online“ zitiert am 16. Juli 2011 aus internen Untersuchungsberichten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie des Zolls, wonach Angriffe der Hackergruppe auf Server der Bundespolizei bereits vor ca. einem Jahr erfolgt seien. Das BSI geht davon aus, dass alle für den Betrieb von Patras bei den unterschiedlichsten Dienststellen unterhaltenen Server kompromittiert seien. Es seien „Trojaner“ auf die nur unzureichend abgesicherten Rechner der Bundespolizei eingeschleust worden, welche das Patras-System als verantwortlicher Dienstleisterin für andere Behörden betreibt. Ferner sei die von der Bundespolizei den Partnerbehörden zur Verfügung gestellte Software zur Absicherung der Server für die Erfüllung dieses Zweckes ungeeignet. Auch die Handlungsanweisungen für den Betrieb der Patras-Datenbank sollen in keinster Weise gängigen Sicherheitsstandards entsprochen haben. Das Ausmaß der erlangten Daten und Informationen aus dem Zuständigkeitsbereich sowohl von Bundespolizei, Bundeskriminalamt und Zoll ist somit bis heute weitgehend ungeklärt. Zwischenzeitlich wurde gemeldet, es seien zwei von drei bereits identifizierten Tatverdächtigen festgenommen worden, einer sei geständig (sueddeutsche.de vom 18. Juli 2011). Laut Meldungen vom 9. August 2011 (unter anderen SPIEGEL ONLINE) soll bereits vor zwei Jahren der private Rechner eines Zollbeamten mit einem Trojaner infiziert worden sein. Dieser habe eine dauerhafte Mailumleitung von seiner dienstlichen Adresse auf seine private Mailadresse vorgenommen, so dass sämtliche dienstlich erhaltenen Informationen dem Zugriff durch Unbefugte offenstanden.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 8. September 2011 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Vorbemerkung der Bundesregierung

Die sogenannte No-Name-Crew hat am 7. Juli 2011, um 18.04 Uhr, in einem Bekennerschreiben an das „Hamburger Abendblatt" die Veröffentlichung von Daten der Bundespolizei angekündigt. Am 7. Juli 2011 gegen 23.40 Uhr erschienen auf der Webseite der „No-Name-Crew" Softwarepakete und dazugehörige Anwendungshinweise sowie Einsatzdaten aus einem Zielverfolgungssystem „Paip-Tracking-Server" (PATRAS). Mit diesem Geoinformationssystem können berechtigte Nutzer die Standorte der Zielverfolgungseinheiten (GPS-Tracking Units) feststellen und dokumentieren. Diese Geo-Daten sind mittels einer kartengestützten Webanwendung grafisch darstellbar.

Nach Bekanntwerden des Sicherheitsvorfalls wurden alle eingesetzten PATRAS-Systeme unverzüglich vom Netz getrennt und abgeschaltet.

Am 16. Juli 2011 wurde in einer ergänzenden Veröffentlichung der „No-Name-Crew" nach derzeitiger Erkenntnislage die unzutreffende Behauptung aufgestellt, man habe ein Jahr lang den Netzwerkverkehr des BKA, der Bundespolizei und des Zolls mitgeschnitten.

Die forensische Untersuchung der abgeschalteten Server sowie der im Rahmen der Ermittlungen sichergestellten Daten dauert an. Nach derzeitigem Stand der Ermittlungen sind jedoch keine Netzwerke der Sicherheitsbehörden kompromittiert worden.

1. Wie viele sicherheitsrelevante Zwischenfälle bei Bundespolizei-, Zoll- und Sicherheitsbehörden kann die Bundesregierung für die zurückliegenden drei Jahre bis heute bestätigen, bei denen nicht ausgeschlossen werden kann, dass personenbezogene und/oder sicherheitsrelevante Daten und Informationen aus dem Bereich dieser Stellen für den Zugriff unbefugter Dritter offenstanden?

Bei der Bundespolizei kam es in den zurückliegenden drei Jahren zu zwei sicherheitsrelevanten Vorfällen (Angriff auf das PATRAS-System und Kompromittierung des privaten Rechners eines Bundespolizisten), bei denen Informationen aus dem Bereich der Bundespolizei für Dritte verfügbar gewesen sein könnten.

Der Zollfahndungsdienst betrieb an zwei Standorten jeweils einen PATRAS-Server.

Beide Server wurden von unbefugten Dritten mit Schadsoftware kompromittiert.

Im Bundeskriminalamt gab es für die zurückliegenden drei Jahre keine Zwischenfälle, bei denen sicherheitsrelevante und/oder personenbezogene Daten und Informationen für den Zugriff unbefugter Dritter offen standen.

2. Welche Stellen des Bundes und/oder der Länder waren bzw. sind von den oben genannten, jüngsten Angriffen konkret betroffen?

Nach derzeitigem Stand der Ermittlungen waren im Bereich des Bundes der Zollfahndungsdienst und die Bundespolizei von den jüngsten Angriffen betroffen.

Darüber hinaus sind nach Kenntnis der Bundesregierung vier Bundesländer gleichartigen Angriffen ausgesetzt gewesen. Die Bundesregierung hat zu diesen außerhalb ihres Verantwortungsbereichs liegenden Systemen der Bundesländer keine detaillierten Erkenntnisse.

3. Seit wann ist der Bundesregierung bzw. den zuständigen Stellen bekannt, dass ein entsprechender Einbruch in das System stattgefunden hat bzw. die Möglichkeit dazu bestand?

Die „No-Name-Crew“ hatte am 7. Juli 2011, um 18.04 Uhr, in einem Bekennerschreiben an das „Hamburger Abendblatt“ die Veröffentlichung von Daten der Bundespolizei angekündigt. Durch das „Hamburger Abendblatt“ wurde die Bundespolizei informiert, die wiederum das Bundesministerium des Innern und das Bundesamt für Sicherheit in der Informationstechnik über den Sachverhalt unterrichtete.

4. Hinsichtlich welcher konkreten Daten und Informationen aus dem Bereich dieser Behörden kann bestätigt bzw. nicht ausgeschlossen werden, dass diese, wenn auch nur vorübergehend, dem Zugriff der Angreifer offenstanden?

Nach derzeitigem Stand der Ermittlungen handelt es sich um Softwarepakete und Servicemitteilungen zur Installation von PATRAS-Servern der Bundespolizei, die ohne notwendigen Freischaltschlüssel nicht verwendet werden können. Aus dem Bereich des Zollfahndungsdienstes konnten anonyme GPS-Tracking Daten, die Anwahlnummern der eingesetzten Peilsender, Verzeichnisnamen sowie die Bezeichnung der sachbearbeitenden Dienststellen eingesehen werden. In einem Fall wurden dazu gehörige Kfz-Kennzeichen und der PKW-Typ ausgelesen, die irrtümlich auf dem Server abgelegt waren.

Hinsichtlich der Weiterleitung dienstlicher E-Mails an ein privates E-Mail-Postfach hatten die Tatverdächtigen über einen längeren Zeitraum Zugang zu dem privaten Rechner eines Bundespolizisten, welcher sich weisungswidrig dienstliche Dateien an sein privates E-Mail-Postfach weitergeleitet hat. Dadurch standen den Angreifern zeitweise lokal begrenzte Dienststelleninformationen (Organisationspläne, Dienstanweisungen, Formulare) zur Verfügung. Diese E-Mailweiterleitung stand in keinem direkten Zusammenhang mit dem PATRAS-Sicherheitsvorfall.

5. Hinsichtlich welcher konkreten Daten und Informationen kann bestätigt werden, dass diese, wenn auch gegebenenfalls nur vorübergehend, im Internet zum Abruf zur Verfügung standen?

Im Internet sind durch die Veröffentlichung der „No-Name-Crew“ die in der Antwort zu Frage 4 dargestellten Daten veröffentlicht worden. Sie standen dort zeitweise für einen Download zur Verfügung.

Zusätzlich wurden aus den in der Antwort zu Frage 4 erwähnten Umständen vier Dokumente aus dem Bereich der Bundespolizeidirektion Koblenz (Bundespolizeiinspektion Frankfurt/Main Bahnhof) aus dem Jahr 2009 veröffentlicht.

6. Auf welche Weise hat sich nach Auffassung der Bundesregierung der Angriff auf Server des Zolls und der Bundespolizei zugetragen?

Die PATRAS-Systeme des Zollfahndungsdienstes bzw. der Bundespolizei wurden über einen automatischen softwarebasierten Scan auf definierte Schwachstellen des Datenbankadministrationssystems ausfindig gemacht. Dabei wurde eine bestehende Sicherheitslücke in der Anwendung „phpMyAdmin“ für einen Zugriff auf die Systeme ausgenutzt. Diese Zugriffsmöglichkeit wurde über Dritte an die „No-Name-Crew“ herangetragen, die sie für eigene Zwecke (Erhöhung des Bekanntheitsgrades) ausnutzte.

Zusätzlich hat die „No-Name-Crew“ aus den in der Antwort zu Frage 4 erwähnten Umständen vier Dokumente aus dem Bereich der Bundespolizeiinspektion Frankfurt/Main Bahnhof aus dem Jahr 2009 veröffentlicht, um den Eindruck zu erwecken, ihr wäre ein umfangreicher Einbruch in die internen Netze der Bundespolizei gelungen.

7. Welche Behörde bzw. welches Bundesministerium zeichnet für die Ausermittlung der jüngst gemeldeten Angriffe auf Server des Zolls sowie der Bundespolizei verantwortlich?

Aufgrund der Strafanzeigen des Zollkriminalamtes (ZKA) und der Bundespolizei hat die Staatsanwaltschaft (StA) Karlsruhe (zuständig für den Standort des angegriffenen PATRAS-Rechners des ZKA) ein Ermittlungsverfahren eröffnet und das Bundeskriminalamt (BKA) mit den bundesweiten Ermittlungen beauftragt. Dieses Verfahren wurde später an die für den Wohnort des ermittelten Tatverdächtigen zuständige StA Würzburg abgegeben. Hinsichtlich eines weiteren Tatverdächtigen wurde ein zusätzliches Verfahren bei der StA Detmold eröffnet. Parallel hierzu führt die StA Köln ein Ermittlungsverfahren wegen eines Angriffs auf PATRAS-Systeme der Polizei Nordrhein-Westfalen, bei welchen das Landeskriminalamt Nordrhein-Westfalen mit den Ermittlungen beauftragt wurde. Entsprechend der Absprache der beteiligten Staatsanwaltschaften ist Gegenstand der Ermittlung der StA Würzburg der Angriff auf die Server des Zolls und der Bundespolizei und die Weitergabe der gewonnenen Daten an die „No-Name-Crew“, während durch die StA Köln die Nutzung der herangetragenen Daten sowie weitere durch die „No-Name-Crew“ begangene Straftaten ermittelt werden.

Im Hinblick auf IT-Sicherheit und Schlussfolgerungen/Prävention werden die Ermittlungsergebnisse jedoch auch von den zuständigen Ressorts, Bundesministerium des Innern und Bundesministerium der Finanzen, weiterhin verfolgt und bewertet.

8. Zu welchem Zeitpunkt und mit welcher konkreten Aufgabenstellung bzw. mit welchem konkreten Ziel wurde das neu geschaffene Cyber-Abwehrzentrum eingeschaltet?

   Welche konkreten Ergebnisse hat die Einbeziehung des Cyber-Abwehrzentrums bei der Aufklärung der Vorfälle ergeben?

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) wurde am 8. Juli 2011 in den Vorfall eingeschaltet. Die Aufgabe des Cyber-AZ ist, alle Beteiligten mit den notwendigen Informationen zu versorgen.

In diesem Fall hat das Cyber-AZ alle verfügbaren Informationen über den Vorfall und die Hackergruppe „No-Name-Crew“ zusammengetragen und diese den beteiligten Behörden zur Verfügung gestellt.

9. Zu welchem Zeitpunkt fanden erstmalig Angriffe auf Server bundesdeutscher Behörden statt, die der Gruppe „No-Name-Crew“ zugerechnet werden?

Zum gegenwärtigen Zeitpunkt können der „No-Name Crew“ außer dem Angriff auf die PATRAS-Systeme keine weiteren Angriffe auf Server bundesdeutscher Behörden zugeordnet werden. Nach derzeitigem Stand der Ermittlungen hat die „No-Name-Crew“ die Zugangsdaten von anderen Hackern bekommen und im Juni 2011 erstmalig auf die PATRAS-Systeme zugegriffen.

10. Zu welchem Zeitpunkt fand der Angriff statt, der den oben bezeichneten Zugriff auf das sogenannte Patras-System ermöglichte?

Die Ermittlungen zum Angriff auf die PATRAS-Systeme der Bundespolizei und der Zollfahndung sind noch nicht abgeschlossen. Nach jetzigem Stand wurden die eingesetzten Server erstmalig am 8. September 2010 kompromittiert. Mindestens seit dem 25. Mai 2011 sind Daten von den Systemen heruntergeladen worden.

11. Kann die Bundesregierung ausschließen, dass bei den eingangs beschriebenen Vorgängen auch Daten und Informationen, die nachvollziehbare personenbeziehbare Hinweise auf verdeckt durchgeführte Ermittlungsvorgänge gegen Tatverdächtige im Rahmen des Einsatzes von Patras enthalten, für Unbefugte zugänglich geworden sind?

    Wenn nein, mussten bereits entsprechende Konsequenzen beobachtet werden oder selbst gezogen werden, wie z. B. die Aufhebung der Tarnung von Ermittlern oder der Abbruch von Ermittlungen, zum Schutz von verdeckt tätigen Mitarbeitern?

Nach den bisherigen Erkenntnissen sind keine Einsatzdaten der Bundespolizei kompromittiert worden. Zudem lassen sich aus den im PATRAS-System der Bundespolizei vorgehaltenen Daten durch Unbefugte keine Zusammenhänge zu Verfahren oder Ermittlungen herstellen.

Im Bereich des Zollfahndungsdienstes sind anonyme Geo-Daten aus Peil- und Ortungsmaßnahmen entwendet worden. Die Verknüpfung der Positionsdaten mit dem konkreten Ermittlungsverfahren durch die ermittelnde Dienststelle erfolgt ausschließlich über andere, nicht mit dem Zielverfolgungssystem „PATRAS“ verbundene und besonders geschützte Informationssysteme des Zollfahndungsdienstes. In einem Fall (siehe Antwort zu Frage 4) wurden irrtümlich personenbezogene Daten in einem Protokoll auf dem betroffenen Server abgelegt.

Die betreffenden Ermittlungsverfahren des Zollfahndungsdienstes sind überwiegend bereits abgeschlossen. Es ist davon auszugehen, dass keine laufenden Ermittlungen gefährdet sind. Es mussten daher keine Ermittlungen abgebrochen werden.

12. Ist es zutreffend, dass das gesamte Peil- und Ortungssystem Patras aufgrund des Angriffs und des unklaren Ausmaßes der Betroffenheit der IT-Systeme vorübergehend abgeschaltet werden musste?

    Wenn ja, für welchen Zeitraum und mit welchen konkreten Konsequenzen für die ermittelnden Behörden bzw. die einzelnen zu diesem Zeitpunkt über das System laufenden Vorgänge bzw. Ermittlungen?

Alle eingesetzten PATRAS-Zielverfolgungssysteme wurden vorsorglich abgeschaltet und die vorhandenen Daten gesichert. Diese Abschaltung der Systeme dauert bis auf weiteres an.

Die Ermittlungen mit Zielverfolgung können, allerdings mit höherem Aufwand weitergeführt werden.

13. Auf welche Weise und durch welche Stellen wurde nach Bekanntwerden versucht, den Tathergang aufzuklären, und ist dies nach Ansicht der Bun-

desregierung inzwischen in einem zufriedenstellenden Ausmaß gelungen?

Das ZKA und die Bundespolizei haben Strafanzeigen gegen Unbekannt gestellt. Durch die jeweils zuständigen Staatsanwaltschaften wurden das BKA und das Landeskriminalamt Nordrhein-Westfalen mit den Ermittlungen beauftragt. Diese Ermittlungen werden in enger Abstimmung zwischen allen beteiligten Behörden durchgeführt.

Das Bundesamt für die Sicherheit in der Informationstechnik hat in Zusammenarbeit mit den betroffenen Behörden die computerforensische Untersuchung der eingesetzten Technik vorgenommen.

Die Ermittlungen der Staatsanwaltschaft sowie die damit im Zusammenhang stehenden forensischen Auswertungen der beschlagnahmten Computertechnik dauern an; daher kann zum laufenden Verfahren keine Auskunft gegeben werden.

14. Welchen Anteil an der Aufklärung hat das Geständnis des 23-jährigen, vorübergehend festgenommenen mutmaßlichen Täters?

Hierzu kann die Bundesregierung keine Aussage machen. Es wird Aufgabe der Justiz sein, das Geständnis – ggf. im Rahmen der freien Beweiswürdigung – in die Beurteilung des gesamten Sachverhaltes einfließen zu lassen.

15. Waren nach Einschätzung der Bundesregierung für die Tatausführung überdurchschnittliche Fähigkeiten und/oder Erfahrungen erforderlich, oder genügten angesichts der von den Tätern angetroffenen Sicherheitsvorkehrungen im Wesentlichen durchschnittliche Kenntnisse, wie sie beispielsweise in einschlägigen Foren etc. vermittelt werden?

Beim Angriff auf die Bundespolizei/den Zollfahndungsdienst waren verschiedene Tätergruppen mit unterschiedlichen, teils überdurchschnittlichen Fähigkeiten beteiligt. Schlussendlich waren für die eigentliche Ausnutzung der dann identifizierten Schwachstellen lediglich durchschnittliche Fähigkeiten ausreichend.

16. Wird der Bericht des Bundesamtes für Sicherheit in der Informationstechnik über den Hergang in dem dafür erforderlichen Umfang zur Information der Öffentlichkeit zur Verfügung gestellt?

    Wenn nein, weshalb nicht?

Der Bericht wird nicht veröffentlicht; er ist als Verschlusssache (VS – Nur für den Dienstgebrauch) eingestuft. Eine Veröffentlichung kann für die Sicherheitsinteressen des Bundes nachteilig sein.

17. Teilt die Bundesregierung die Auffassung, dass auch öffentliche Stellen, wie es etwa der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, kürzlich forderte und es jüngst in Schleswig-Holstein gesetzlich geregelt wurde, einer Informationspflicht bei Sicherheitsvorfällen zumindest gegenüber den Datenschutzbehörden unterliegen sollten?

Wenn nein, was spricht aus Sicht der Bundesregierung gegen eine auf diese Weise mögliche unabhängige Drittkontrolle der vorgenommenen Sicherheitsvorkehrungen verantwortlicher Stellen?

Die Frage zielt auf eine Erweiterung der Regelung des § 42a des Bundesdatenschutzgesetzes (BDSG), die eine umfangreiche Informationspflicht für eine nicht-öffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 BDSG bei unrechtmäßiger Kenntniserlangung von Daten vorsieht, auf alle öffentlichen Stellen des Bundes. § 42a BDSG ist erst am 1. September 2009 in Kraft getreten. Gemäß § 48 Satz 1 BDSG muss die Bundesregierung dem Deutschen Bundestag bis zum 31. Dezember 2012 u. a. über die Auswirkungen des § 42a BDSG berichten. Im Hinblick hierauf ist es verfrüht, jetzt bereits Aussagen zu einem eventuellen Änderungsbedarf des § 42a BDSG zu treffen.

18. Auf welche Weise ist das Zielinformationssystem Patras informationstechnisch in die IT-Infrastruktur integriert?

    Welche Behörden haben auf welcher Rechtsgrundlage Zugriffs- bzw. Nutzungsrechte?

Die PATRAS-Systeme der Bundespolizei und des Zollfahndungsdienstes waren „Standalone"-Systeme, die sich nicht innerhalb der jeweiligen IKT-Netze der Behörden befanden. Daher wurden keine weiteren Systeme der Bundespolizei und des Zollfahndungsdienstes kompromittiert.

Das von der Bundespolizei betriebene PATRAS-System wurde nur von der Bundespolizei genutzt. Andere Behörden haben in ihrem Zuständigkeitsbereich im Rahmen eigener Befugnisse eigene PATRAS-Systeme betrieben.

19. Wer ist die datenschutzrechtlich verantwortliche Stelle für den Betrieb des Patras-Systems, und in welchem Umfang werden welche Arten von personenbezogenen Daten in Patras bzw. der dafür geschaffenen Infrastruktur gespeichert?

    Ist es zutreffend, dass die Bundespolizei datenschutzrechtlich im Sinne eines Auftragnehmers einer Auftragsdatenverarbeitung tätig wird?

Alle Nutzer des Zielverfolgungssystems PATRAS haben eigene Server für ihre Ermittlungen betrieben und sind damit eigenverantwortlich für die Umsetzung der datenschutzrechtlichen Bestimmungen.

Datenschutzrechtlich verantwortliche Stelle für den angegriffenen Server der Bundespolizei ist das Bundespolizeipräsidium.

Es werden keine personenbezogenen Daten gemäß § 3 Absatz 1 BDSG im PATRAS-System der Bundespolizei verarbeitet oder gespeichert.

Der angegriffene Server des Zollfahndungsdienstes wird vom Zollkriminalamt betrieben, das somit auch die datenschutzrechtlich verantwortliche Stelle ist. Dieser GPS-Server des Zollfahndungsdienstes diente jedoch ausschließlich der Anwendung zur Peilung und Ortung von Zielobjekten durch Spezialeinheiten. Es wurden dabei anonyme, grundsätzlich nicht personenbezogene Daten für den Zollfahndungsdienst erhoben, verarbeitet oder genutzt. Die Verknüpfung der erhobenen Positionsdaten mit einem konkreten Ermittlungsverfahren erfolgte erst durch die ermittlungsführende Dienststelle über andere nicht mit dem GPS-Server verbundene und besonders geschützte Informationssysteme.

Da jede Behörde eigene PATRAS-Systeme zur Unterstützung ihrer Ermittlungen eingesetzt hat, wird die Bundespolizei hier nicht als Auftragnehmer für eine Auftragsdatenverarbeitung gemäß § 11 Absatz 1 BDSG tätig.

20. Welche Verantwortlichkeiten für IT-Sicherheit und Datenschutz beim Einsatz des Patras-Systems treffen nach Auffassung der Bundesregierung die ebenfalls mitnutzenden Landeskriminalämter (LKA), das Bundeskriminalamt sowie den Zoll bzw. das Zollkriminalamt?

    Sind nach Auffassung der Bundesregierung insoweit alle das System einsetzenden Stellen den Vorgaben entsprechend ordnungsgemäß vorgegangen?

Jeder Nutzer von PATRAS betreibt eigenverantwortlich ein PATRAS-System und ist somit auch für die IT-Sicherheit und den Datenschutz verantwortliche Stelle. Das BKA nutzt kein PATRAS-System.

Da die Untersuchungen zu den Angriffen auf die PATRAS-Systeme noch nicht beendet sind, kann hierzu noch nicht abschließend Stellung genommen werden.

Der Vorfall wird aber zum Anlass genommen, die bisherigen Sicherheitskonzepte für die Informations- und Kommunikationsinfrastruktur und deren Umsetzung auf den Prüfstand zu stellen. Dabei sind auch die Sicherheitsstrukturen sowie die Informations- und Meldewege zu überprüfen und gegebenenfalls anzupassen. Über weitergehende Maßnahmen wird nach Abschluss der Schwachstellenanalyse entschieden.

21. Ist es zutreffend, dass in der Bundespolizeikaserne Swisstal-Heimerzheim ein zentraler Server für den Betrieb von Patras steht, welcher über das Internet mit den weiteren, das System einsetzenden Behörden (LKA, BKA, Zoll) verbunden ist?

    Wurde nach Kenntnis der Bundesregierung auch dieser Server durch Trojaner befallen, und wenn ja, zu welchem Zeitpunkt?

Im Bundespolizei-Standort Swisttal-Heimerzheim wurde ein zentraler Server für die Zielverfolgung der Bundespolizei sowie für die Bereitstellung der Softwarepakete (Downloadserver) zur Installation von PATRAS-Systemen betrieben.

Für die Bundespolizei war der Downloadserver von der Kompromittierung mit Schadsoftware betroffen. Lediglich zu diesem Downloadserver von PATRAS hatten andere Behörden temporären Zugriff. Eine Sicherheitslücke im verwendeten Datenbankverwaltungsprogramm „phpMyAdmin“ erlaubte, wie bereits in der Antwort zu Frage 6 dargestellt, das Einschleusen von Schadsoftware und somit den illegalen Zugriff auf den Server.

22. Welche Sicherheitsvorkehrungen sieht die Bundespolizei generell für den Schutz ihrer Netzwerke vor Angriffen aus dem Internet vor?

Die Netzwerke der Bundespolizei (BPOLNET) sind nicht direkt mit dem Internet verbunden. Das BPOLNET hat nur Übergänge in die sicheren Behördennetze (IVBB/BVN) und das Corporate Network der Polizeien (CNP).

Übergänge zu Netzen Dritter sind mit einer dreistufigen Firewall abzusichern.

23. Welche Systeme werden über das Internet mit anderen Behörden verbunden, und welche Sicherheitsvorgaben bestehen für die Anbindung über das Internet?

IT-Systeme der Bundespolizei werden nicht mit anderen Behörden über das Internet verbunden. Im Übrigen wird auf die Antwort zu Frage 22 verwiesen.

24. Bestehen bei Bundespolizei, Zoll und Bundeskriminalamt Sicherheitsvorgaben für die Inbetriebnahme eines Programmes wie Patras?

    Wenn ja, welche?

Für diese Systeme der Sonderinformations- und Kommunikationstechnik bei den genannten Behörden gibt es jeweils Sicherheitsvorgaben auf Basis der Grundschutzvorgaben des BSI.

25. Wurden für Patras Vorabkontrollen und/oder Erlaubnisverfahren durch das BSI und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durchgeführt?

    Wenn nein, weshalb nicht?

Bei den angegriffenen PATRAS-Systemen der Bundespolizei und des Zollfahndungsdienstes gab es bisher keine Vorabkontrollen und/oder Erlaubnisverfahren durch das BSI. Nach Abschluss der Ermittlungen ist vorgesehen, das PATRAS-System neu zu konfigurieren. Eine Überprüfung der neuen PATRAS-Systeme durch das BSI ist vorgesehen.

Da in PATRAS keine personenbezogenen Daten verarbeitet werden sollen, wurde von einer Beteiligung des Bundesbeauftragten für Datenschutz abgesehen.

26. Hat es in der Vergangenheit bereits unabhängige Prüfungen des Wirkbetriebes von Patras seitens des BSI und/oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gegeben?

    Ist jetzt eine entsprechende Prüfung vorgesehen?

Bei den angegriffenen PATRAS-Systemen der Bundespolizei und des Zollfahndungsdienstes gab es bisher keine unabhängigen Überprüfungen des Wirkbetriebes durch das BSI. Nach Abschluss der Ermittlungen ist vorgesehen, das PATRAS-System neu zu konfigurieren. Eine Überprüfung der neuen PATRAS-Systeme durch das BSI ist vorgesehen.

27. Wie konnten aus Sicht der Bundesregierung die entsprechenden Schadprogramme die Schutzvorkehrungen bei der Bundespolizei bzw. den angeschlossenen Behörden überwinden?

Wie in der Antwort zu Frage 6 schon ausgeführt, wurden die PATRAS-Systeme des Zollfahndungsdienstes bzw. der Bundespolizei über einen automatischen softwarebasierten Scan auf definierte Schwachstellen des Datenbankadministrationssystems ausfindig gemacht. Dabei wurde eine bestehende Sicherheitslücke in der Anwendung „phpMyAdmin“ für einen Zugriff auf die Systeme ausgenutzt.

28. Hat die Bundespolizei verantwortlich Sicherheitssoftware für den Betrieb von Patras an die beteiligten Behörden ausgeliefert, und wenn ja, welche?

    Handelte es sich dabei um das in diesem Zusammenhang von mehreren Quellen unter anderem auch im Internet unabhängig voneinander erwähnte Programm XAMP?

Die Bundespolizei hat mit PATRAS ein XAMPP-Paket für das Betriebssystem Windows ausgeliefert. Bei XAMPP handelt es sich um eine Zusammenstellung

von freier Software. XAMPP ermöglicht das einfache Installieren und Konfigurieren des Webservers Apache mit der Datenbank MySQL bzw. SQLite und den Skriptsprachen Perl und PHP. Es handelt sich bei XAMPP nicht um eine Sicherheitssoftware. Die Nutzung von XAMPP ist für den Betrieb von PATRAS nicht notwendig. Die Bundespolizei hat XAMPP bei PATRAS lediglich mitgeliefert, um den nutzenden Behörden die Inbetriebnahme zu erleichtern.

29. Wie bewertet die Bundesregierung die Tatsache, dass die Bundespolizei dieses Programm zum Einsatz brachte bzw. den beteiligten Behörden zur Absicherung empfahl, dass selbst von Zollbeamten und der Bundesnetzagentur für diesen Zweck für ungeeignet gehalten wird?

Der Bundesregierung sind die dargestellten Bedenken der Bundesnetzagentur nicht bekannt. Bedenken des ZKA wurden im Zusammenhang mit der Analyse der Angriffe auf die PATRAS-Systeme an das BMF berichtet.

30. Lagen konkrete Handlungsanweisungen für den Einsatz von Patras durch Behörden seitens der Bundespolizei vor?

    Wenn ja, wurde dort die datenbankmäßige Speicherung von Passwörtern im Klartext nahegelegt?

    Sollte dies der Fall gewesen sein, wie bewertet die Bundesregierung eine derartige Vorgabe?

Die Bundespolizei hat dem Installationspaket für die PATRAS-Systeme auch ein Handbuch mit entsprechenden Handlungsanweisungen beigefügt.

Eine datenbankmäßige Speicherung von Passwörtern im Klartext wurde in den Handlungsanweisungen nicht nahegelegt.

31. Seit wann ist der Bundesregierung bzw. den zuständigen Stellen bekannt, dass aufgrund einer Mailumleitung auf den Privatrechner eines Zollmitarbeiters dienstliche Informationen für unbefugte Dritte zugänglich waren?

Im Rahmen der Ermittlungen in Zusammenhang mit den Aktivitäten der „No-Name-Crew“ wurde am 18. Juli 2011 bekannt, dass ein Beamter der Bundespolizei über einen längeren Zeitraum dienstliche E-Mails an sein privates E-Mailpostfach weitergeleitet hat. Bei einer durch die StA Köln angeordneten Durchsuchung der privaten Wohnung des Beamten der Bundespolizei gemäß § 103 der Strafprozessordnung (StPO) wurde am 24. Juli 2011 u. a. der private Rechner des Beamten sichergestellt.

Derzeit ist kein Fall bekannt, in dem aufgrund einer Mailumleitung auf den Privatrechner eines Zollbeamten dienstliche Informationen für unbefugte Dritte zugänglich waren.

32. Für welchen Gesamtzeitraum kann nicht ausgeschlossen werden, dass Daten und Informationen dieser Stellen für den Zugriff unbefugter Dritter offenstanden?

Da es sich hier um ein laufendes Ermittlungsverfahren handelt, kann zu diesem Zeitpunkt keine Auskunft darüber gegeben werden.

33. Ist es zutreffend, dass aufgrund des genannten Falles eines Zollmitarbeiters, welcher eine Mailumleitung von seinem dienstlichen auf seinen privaten Rechner vorgenommen hatte, nunmehr einzelne Landeskriminalämter per Dienstanweisung entsprechende Mailumleitungen untersagt haben?

    Wenn ja, um welches LKA handelt es sich?

In Bezug auf die Kompromittierung des privaten Rechners eines Beamten der Bundespolizei wird auf die Antwort zu Frage 31 verwiesen.

Die Bundesregierung hat zu den außerhalb ihres Verantwortungsbereichs liegenden Maßnahmen der Bundesländer keine detaillierten Erkenntnisse.

34. Sind entsprechende Mailumleitungen auch bei anderen polizeilichen Bundesbehörden technisch möglich?

    Welche Regelungen bestehen zu Mailumleitungen auf Bundesebene bei den betroffenen Behörden Bundeskriminalamt, Zoll und Bundespolizei?

Beim BKA, dem Zollfahndungsdienst und bei der Bundespolizei sind E-Mailweiterleitungen an private E-Mailkonten für alle Nutzer untersagt.

Im BKA und dem Zollfahndungsdienst werden automatische Mailumleitungen technisch unterbunden.

In Auswertung dieses Sicherheitsvorfalls wurde bei der Bundespolizei ebenfalls die automatische Mailumleitung technisch unterbunden.

35. Liegt nach Auffassung der Bundesregierung in den vorliegend geschilderten Sachverhalten vorwerfbares Fehlverhalten vor?

    Wer trägt, soweit die geschilderten Sicherheitslücken zutreffen sollten, die Verantwortung dafür, und welche Konsequenzen zieht die Bundesregierung aus diesen Vorgängen?

Die Ermittlungen zu den Sicherheitsvorfällen dauern an. Dienstliche Konsequenzen werden geprüft.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333